



# VPN Tracker for Mac OS X



**How-to:**  
**Interoperability with**  
**NETGEAR FVS318v3**

Rev. 1.0

Copyright © 2005 equinux USA Inc. All rights reserved.

# 1. Introduction

This document describes how VPN Tracker can be used to establish a connection between a Macintosh running Mac OS X and a NETGEAR FVS318v3 Internet Security Appliance.

The NETGEAR FVS318v3 is configured as a router connecting a company LAN to the Internet.

This paper is only a supplement to, not a replacement for, the instructions that have been included with your NETGEAR router. Please be sure to read those instructions and understand them before starting.

All trademarks, product names, company names, logos, screenshots displayed, cited or otherwise indicated on the How-to are the property of their respective owners.

EQUINIX SHALL HAVE ABSOLUTELY NO LIABILITY FOR ANY DIRECT OR INDIRECT, SPECIAL OR OTHER CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE USE OF THE HOW-TO OR ANY CHANGE TO THE ROUTER GENERALLY, INCLUDING WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS, OR DATA, EVEN IF EQUINIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## 2. Prerequisites

First you have to make sure that you use a recent NETGEAR FVS318v3 firmware version. The latest firmware release for your NETGEAR appliance can be obtained from

<http://www.NETGEAR.com/>

For this document, firmware version 3.0\_16 has been used.

**Please note:** Firmware version 3.0\_20 has some issues in conjunction with VPN Tracker.

Please refer for howto documentation of NETGEAR's FVS318 and FVS318v2 models to <http://www.vpntracker.com/interop/>.

When using Pre-shared key authentication you need one VPN Tracker Personal Edition license for each Mac connecting to the NETGEAR.

We recommend one VPN Tracker Professional Edition for the administrator's Mac in order to export configuration files to the clients.

VPN Tracker is compatible with Mac OS X 10.2.5+, 10.3 and 10.4

### 3. Connecting a VPN Tracker host to a NETGEAR FVS318v3

In this example the Mac running VPN Tracker is directly connected to the Internet via a dialup or PPP connection.

The NETGEAR FVS318v3 is configured in NAT mode and has the static WAN IP address 169.1.2.3 and the private LAN IP address 192.168.1.1. The Stations in the LAN behind the NETGEAR router use 192.168.1.1 as their default gateway and should have a working Internet connection.

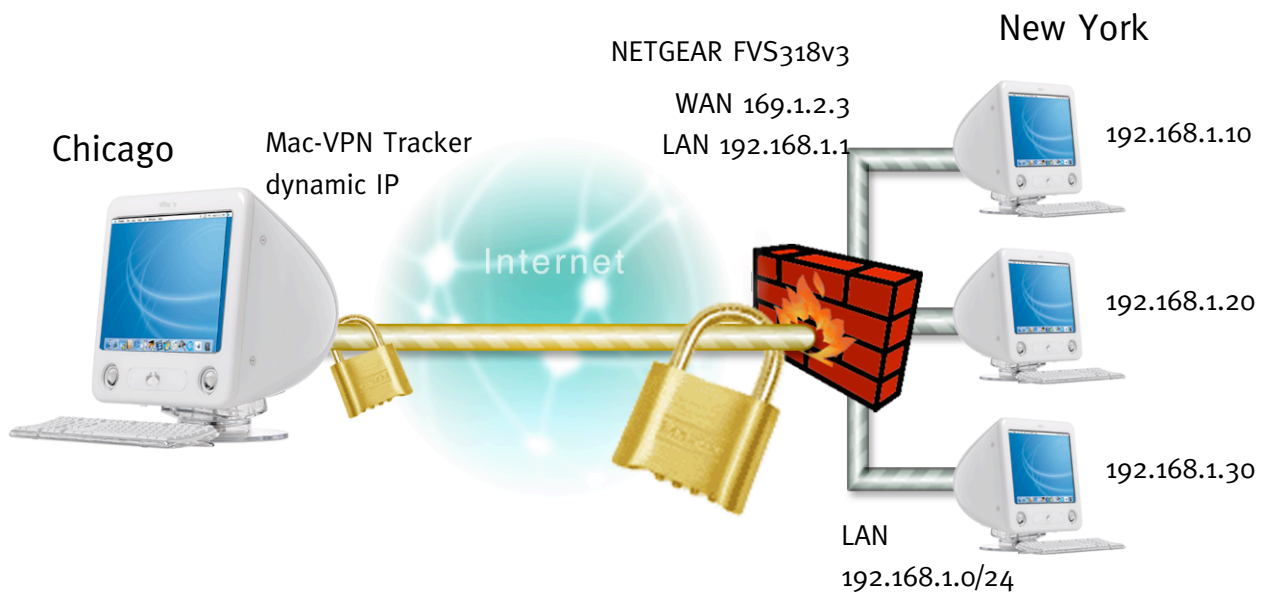


Figure 1: VPN Tracker – NETGEAR FVS318v3 connection diagram

#### 3.1 NETGEAR Configuration

The pre-defined VPN Tracker connection type has been created using the default settings for your NETGEAR FVS318v3 appliance. If you change any of the settings on the NETGEAR router, you will eventually have to adjust the connection type in VPN Tracker.

##### Step 1

Create an IKE Policy with following settings:

- Policy Name: an arbitrary name (e.g. **vpntracker**)
- Direction/Type: **Remote Access**
- Exchange Mode: **Aggressive**
- Local Identity Type: **Fully Qualified Domain Name**
- Local Identity Data: an arbitrary identifier (e.g. **netgear**)
- Remote Identity Type: **Fully Qualified Domain Name**
- Remote Identity Data: an arbitrary identifier (e.g. **vpntracker**)
- Encryption Algorithm: **3DES**
- Authentication Algorithm: **MD5**
- Pre-shared Key: an arbitrary key (e.g **secretkey**)

The screenshot shows the NETGEAR ProSafe VPN Firewall FVS318v3 settings page. The left sidebar contains a navigation menu with categories: Setup (Setup Wizard, Basic Settings, Logs, Block Sites, Rules, Services, Schedule, E-mail), VPN (VPN Wizard, IKE Policies, VPN Policies, CAs, Certificates, CRL, VPN Status), Maintenance (Router Status, Attached Devices, Settings Backup, Set Password, Diagnostics, Router Upgrade), Advanced (Dynamic DNS, LAN Setup, Remote Management, Static Routes), and Web Support (Knowledge Base, Documentation). The main content area is titled 'IKE Policy Configuration' and contains the following fields:

- General**
  - Policy Name: vpntracker
  - Direction/Type: Remote Access
  - Exchange Mode: Aggressive Mode
- Local**
  - Local Identity Type: Fully Qualified Domain Name
  - Local Identity Data: netgear
- Remote**
  - Remote Identity Type: Fully Qualified Domain Name
  - Remote Identity Data: vpntracker
- IKE SA Parameters**
  - Encryption Algorithm: 3DES
  - Authentication Algorithm: MD5
  - Authentication Method: Pre-shared Key (selected), RSA Signature (requires Certificate)
  - Diffie-Hellman (DH) Group: Group 1 (768 Bit)
  - SA Life Time: 3600 (secs)

At the bottom of the configuration area are 'Back', 'Apply', and 'Cancel' buttons. On the right side, there is an 'IKE Policy Configuration Help' section with detailed information about IKE, including sections for General, Direction/Type, Exchange Mode, and Local Identity Type.

Figure 2: NETGEAR FVS318v3 - IKE Policy Configuration

### 3. Connecting a VPN Tracker host to a NETGEAR FVS318v3

#### Step 2

Create a VPN Auto Policy with following settings:

- Policy Name: an arbitrary name (e.g. **autopolicy**)
- IKE policy: your previously create IKE policy (e.g. **vpntracker**)
- Remote VPN Endpoint:
  - Address Type: **IP Address**
  - Address Data: **0.0.0.0**
- Local IP: **Subnet address**
  - Start IP address: network address of the NETGEAR lan (e.g. **192.168.1.0**)
  - Subnet Mask: e.g. **255.255.255.0**
- Remote IP: **Single address**
  - Start IP address: Virtual IP address for the client (e.g. **10.1.2.3**)
- ESP -> Enable Encryption: **3DES**
- ESP -> Enable Authentication: **SHA1**

The screenshot shows the 'VPN - Auto Policy' configuration page in the NETGEAR ProSafe VPN Firewall FVS318v3 web interface. The left sidebar contains navigation links for Setup Wizard, Setup, Basic Settings, Security, Logs, Block Sites, Rules, Services, Schedule, E-mail, VPN, VPN Wizard, IKE Policies, VPN Policies, CAs, Certificates, CRL, VPN Status, Maintenance, Router Status, Attached Devices, Settings Backup, Set Password, Diagnostics, Router Upgrade, Advanced, Dynamic DNS, LAN Setup, Remote Management, and Static Routes, as well as Web Support, Knowledge Base, and Documentation. The main content area is titled 'VPN - Auto Policy' and includes sections for General, Traffic Selector, AH Configuration, ESP Configuration, and PFS. The General section shows Policy Name as 'autopolicy', IKE policy as 'vpntracker', Remote VPN Endpoint as 'IP Address' with Address Data '0.0.0.0', SA Life Time as '3600' seconds, and PFS Key Group as 'Group 1 (768 Bit)'. The Traffic Selector section shows Local IP as 'Subnet address' with Start IP '192.168.1.0' and Subnet Mask '255.255.255.0', and Remote IP as 'Single address' with Start IP '10.1.2.3' and Subnet Mask '0.0.0.0'. The AH Configuration section has 'Enable Authentication' checked and 'Authentication Algorithm' set to 'MD5'. The ESP Configuration section has 'Enable Encryption' and 'Enable Authentication' checked, with 'Encryption Algorithm' set to '3DES' and 'Authentication Algorithm' set to 'SHA-1'. The PFS section has 'NETBIOS Enable' unchecked. A 'VPN Auto Policy Help' sidebar on the right provides detailed information about the policy, including a description of the IKE protocol, instructions for naming the policy, and notes on SA Life Time and PFS. At the bottom of the main content area are 'Back', 'Apply', and 'Cancel' buttons.

NETGEAR Router

NETGEAR ProSafe VPN Firewall FVS318v3

settings

VPN - Auto Policy

**General**

Policy Name: autopolicy

IKE policy: vpntracker

Remote VPN Endpoint: IP Address

Address Data: 0.0.0.0

SA Life Time: 3600 (Seconds)

0 (Kbytes)

☐ IPsec PFS

PFS Key Group: Group 1 (768 Bit)

**Traffic Selector**

Local IP: Subnet address

Start IP address: 192 . 168 . 1 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Remote IP: Single address

Start IP address: 10 . 1 . 2 . 3

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

**AH Configuration**

☐ Enable Authentication

Authentication Algorithm: MD5

**ESP Configuration**

☒ Enable Encryption

Encryption Algorithm: 3DES

☒ Enable Authentication

Authentication Algorithm: SHA-1

☐ NETBIOS Enable

Back Apply Cancel

**VPN Auto Policy Help**

This screen allows you to define or edit an "Auto" VPN policy.

An "Auto" VPN policy uses the IKE (Internet Key Protocol) to exchange and negotiate parameters for the IPsec SA (Security Association). Because of this negotiation, it is not necessary for all settings on this VPN Gateway to match the settings on the remote VPN endpoint. Where settings must match, this is indicated.

**General**

These settings identify this policy and determine its major characteristics.

**Name**

Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.

**IKE policy**

The existing IKE policies are presented in a drop-down list. The required IKE policy must be created BEFORE the VPN policy. Select the desired IKE policy.

**Remote VPN Endpoint**

Select the desired option (IP address or Domain Name) and enter the address of the remote VPN Gateway/Server or client you wish to connect to.

Note: The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".

**SA Life Time**

This determines the time interval before the SA (Security Association) expires. (It will automatically be re-established if necessary.) While using a short time period (or data amount) increases security, it also degrades performance. It is common to use periods over an hour (3600 seconds) for the SA Life Time.

**PFS (Perfect Forward Secrecy)**

If enabled, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. (Each key has no relationship to the previous key.)

PFS Key Group - If PFS is enabled, this setting determines the DH group used.

Figure 3: NETGEAR FVS318v3 - VPN Auto Policy

### 3. Connecting a VPN Tracker host to a NETGEAR FVS318v3

#### ❖ Multiple VPN Tracker Hosts

When connecting with more than one VPN Tracker client, you'll need to repeat step 2 and supply a different "Remote IP", like 10.1.2.4 to the client.

## 3.2 VPN Tracker Configuration

### Step 1

Add a new connection with the following options:

- Vendor: **NETGEAR**
- Model: **NETGEAR FVS318**

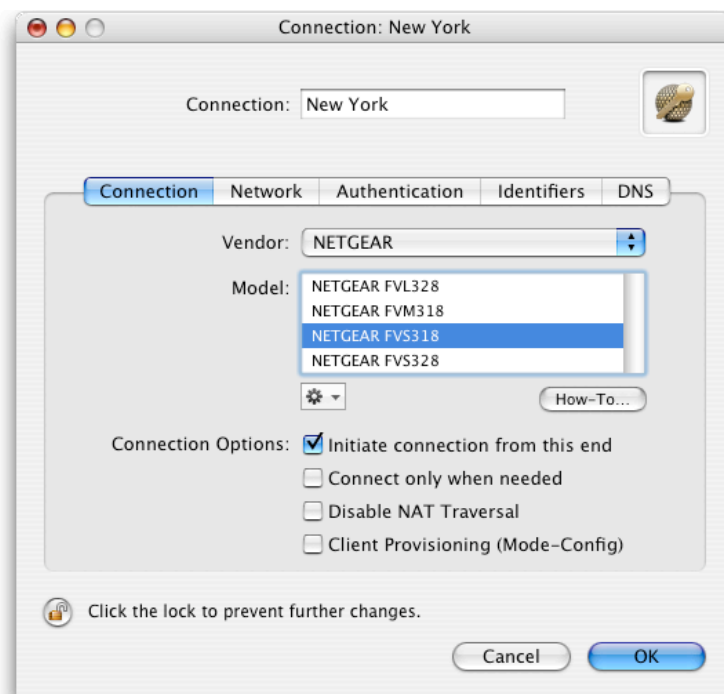


Figure 4: VPN Tracker - Connection Settings

### 3. Connecting a VPN Tracker host to a NETGEAR FVS318v3

#### Step 2

Change your Network Settings:

- VPN Server Address: public IP address of your VPN Gateway (e.g. **169.1.2.3**)
- Local Address: the virtual IP address you've enter in section 3.1 step 2 (e.g. **10.1.2.3**)
- Remote Network/Mask: network address and netmask of the remote network (eg. **192.168.1.0/255.255.255.0**).

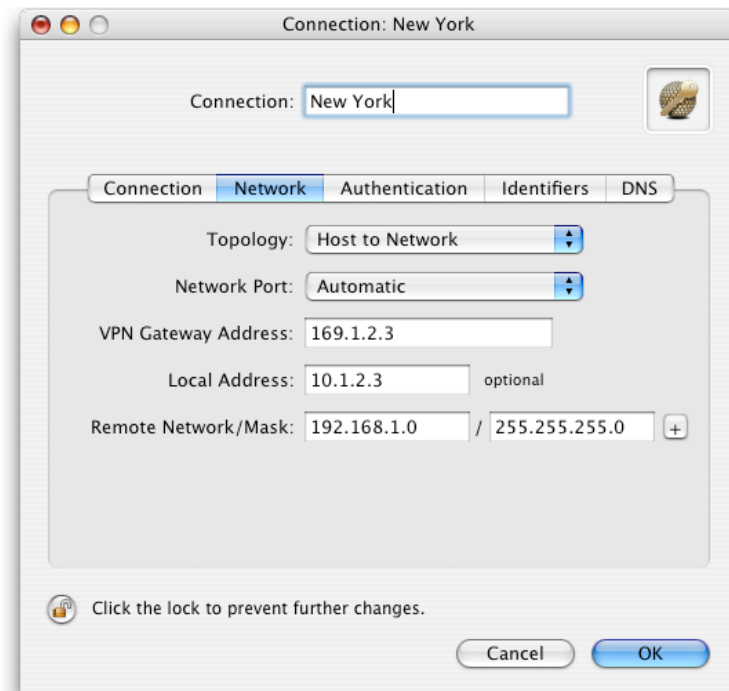


Figure 5: VPN Tracker - Network Settings

**Please note:** The “Local Address” field is required in order to connect to your NETGEAR FVS318v3 router.



### 3. Connecting a VPN Tracker host to a NETGEAR FVS318v3

#### Step 3

Change your Authentication Settings:

Pre-shared key: the same Pre-shared key as in the NETGEAR FVS318v3 configuration.

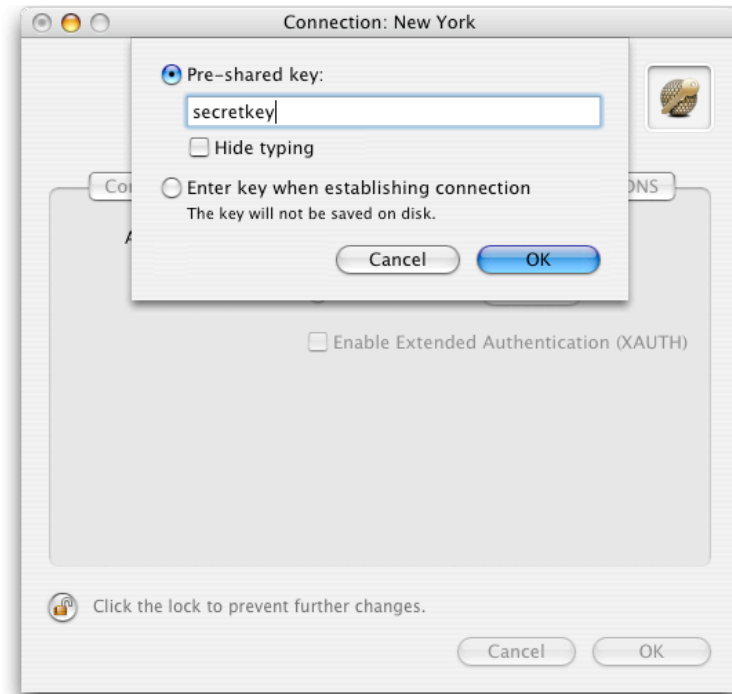


Figure 6: VPN Tracker - Authentication Settings

### 3. Connecting a VPN Tracker host to a NETGEAR FVS318v3

#### Step 4

Identifier Settings:

- Local Identifier: **vpntracker** (identifier type: fqdn).
- Remote Identifier: **netgear** (identifier type: fqdn).

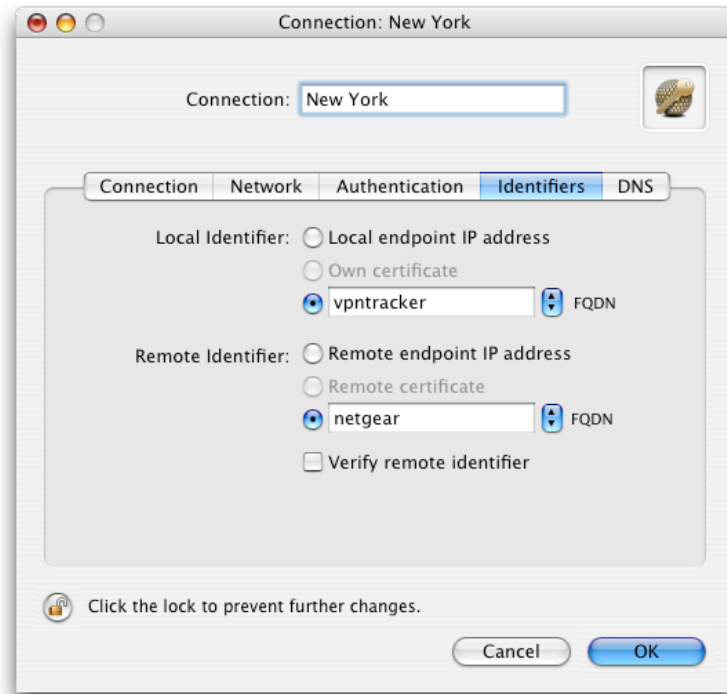


Figure 7: VPN Tracker - Identifier Settings

#### Step 5

Save the connection and Click „Start VPN“ in the VPN Tracker main window.

You're done. After 10-20 seconds the red status indicator for the connection should change to green, which means you're securely connected to the NETGEAR FVS318v3. After IPsec has been started, you may quit VPN Tracker. The IPsec service will keep running.

Now to test your connection simply ping a host in the NETGEAR network from the dialed-in Mac in the "Terminal" utility:

```
ping 192.168.1.10
```